ABSTRACT

A method and apparatus for improving the efficiency of hardware-based binary multiplication. By using radix-32 and radix-256 multipliers where each radix-32 digit is represented by two radix-7 digits and each radix-256 digit is represented by three radix-11 digits, the digit magnitudes are in power of two, which simplifies the implementation of the partial product generation. The partial products depending on multiples of the radices 7 or 11 can be separately accumulated, with multiplication by the radix a pre- or post-computation option.